Attorney Docket No. 03-4019

UNITED STATES PATENT APPLICATION

OF

David Spencer PEARSON

Brig Barnum ELLIOTT

FOR

SYSTEMS AND METHODS FOR IMPLEMENTING ROUTING PROTOCOLS AND ALGORITHMS FOR QUANTUM CRYPTOGRAPHIC KEY TRANSPORT

SYSTEMS AND METHODS FOR IMPLEMENTING ROUTING PROTOCOLS AND ALGORITHMS FOR QUANTUM CRYPTOGRAPHIC KEY TRANSPORT

CROSS REFERENCE TO RELATED APPLICATION

[0001] The instant application claims priority from provisional application number 60/456,815 (Attorney Docket No. 03-4019PRO1), filed March 21, 2003, the disclosure of which is incorporated by reference herein in its entirety.

RELATED APPLICATIONS

[0002] The present application is related to U.S. Patent Application No. _____ (Attorney Docket No. 03-4018), entitled "Systems and Methods for Implementing Routing Protocols for Quantum Cryptographic Key Transport," and filed on a same date herewith; and U.S. Patent Application No. 09/611,783 (Attorney Docket No. 99-449), entitled "Systems and Methods for Implementing a Quantum-Cryptographic Communications Network," and filed on July 2, 2000, the disclosures of which are incorporated by reference herein in their entirety.

GOVERNMENT CONTRACT

[0003] The U.S. Government has a paid-up license in this invention and the right in limited circumstances to require the patent owner to license others on reasonable terms as provided for by the terms of Contract No. F30602-01-C-0170, awarded by the Defense Advanced Research Projects Agency (DARPA).

FIELD OF THE INVENTION

[0004] The present invention relates generally to cryptographic systems and, more particularly, to systems and methods for implementing routing protocols and algorithms for key transport in quantum cryptographic systems.

BACKGROUND OF THE INVENTION

[0005] Conventional packet-switching networks permit cheap and reliable communications independent of the distance between a source node and a destination node in the network. These conventional networks often rely upon either public keys or shared private keys to provide privacy for messages that pass through the network's links. Public key cryptographic systems have the drawback that they have never been proven to be difficult to decipher. Therefore, it is possible that a method of efficiently cracking public key systems may one day be discovered. Such a discovery could make all public key technology obsolete. All supposedly "secure" networks based on public key technology would thus become vulnerable. Shared private keys also have the drawback that the logistics of distributing the private keys can be prohibitive.

[0006] Quantum cryptography represents a recent technological development that provides for the assured privacy of a communications link. Quantum cryptography is founded upon the laws of quantum physics and permits the detection of eavesdropping across a link. Quantum cryptographic techniques have been conventionally applied to distribute keys from a single photon source to a single photon detector, either through fiber optic strands or through the air. Although this approach is perfectly feasible for scientific experiments, it does not provide the kind of "anyone to anyone" connectivity that is provided by current communications technology. Conventional quantum cryptographic techniques require a direct connection to anyone with whom one wishes to exchange keying material. Obviously, a large system built along these lines would be impractical, since it would require every

person to have enough sources and/or detectors, and fiber strands so that they could employ a dedicated set of equipment for each party with whom they intend to communicate.

[0007] Furthermore, conventional quantum cryptographic techniques fail to adequately handle the situations in which eavesdropping is present on a link or when a dedicated link fails (e.g., a fiber is accidentally cut). In conventional quantum cryptographic techniques, further key distribution across the dedicated link becomes impossible until eavesdropping on the link ceases or the link is repaired. In addition, there may exist situations in which a single quantum cryptographic link may not be able to connect two endpoints, such as, for example, if the distance between the two endpoints causes too much signal attenuation, or because the two endpoints use different, incompatible optical encoding schemes.

[0008] It would, thus, be desirable to implement a quantum cryptographic network that could provide the "any to any" connectivity of conventional packet-switching networks, such as the Internet, while eliminating the need for a direct connection between parties transporting quantum cryptographic key material, and which may further sustain key distribution even with link failure and/or when eavesdropping exists on the link.

[0009] Therefore, there exists a need for systems and methods that combine the assured privacy achieved with quantum cryptography with the distance independent communication achieved with conventional multi-node, multi-link packet switching networks.

SUMMARY OF THE INVENTION

[0010] Systems and methods consistent with the present invention address this and other needs by implementing routing protocols and algorithms in a quantum cryptographic network, that includes multiple nodes, for transporting secret keys from one end of the quantum

cryptographic key distribution (QKD) network to another. Link metrics associated with each link of the QKD network may be determined and then disseminated throughout the network. The link metrics may be determined, in some implementations, based on a number of secret key bits exchanged between each node connected by a respective link. The disseminated link metrics may be used to determine one or more paths through the QKD network for transporting end-to-end keys that can be used by QKD endpoints for encrypting/decrypting data sent across a public channel.

[0011] In accordance with the purpose of the invention as embodied and broadly described herein, a method of transporting keys in a quantum cryptographic key distribution (QKD) network includes determining one or more paths for transporting secret keys, using QKD techniques, across a QKD network. The method further includes transporting the secret keys across the QKD network using the determined one or more paths.

[0012] In a further implementation consistent with the present invention, a method of determining link metrics of quantum cryptographic links connecting a node to neighboring nodes in a quantum cryptographic key distribution (QKD) network is provided. The method includes exchanging secret key bits with each of the neighboring nodes using quantum cryptographic mechanisms via the quantum cryptographic links and determining a respective number of available secret key bits exchanged with each of the neighboring nodes. The method further includes determining link metrics associated with each of the quantum cryptographic links based on the respective number of secret key bits exchanged with each of the neighboring nodes.

[0013] In an additional implementation consistent with the present invention, a method of

determining a link metric for each direction along quantum cryptographic links in a quantum cryptographic key distribution (QKD) network includes exchanging quantities of secret key bits between neighboring nodes in the QKD network using quantum cryptographic mechanisms over the quantum cryptographic links. The method further includes determining link metrics for each direction along each respective quantum cryptographic link of the quantum cryptographic links based on the exchanged quantities of secret key bits.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate exemplary embodiments of the invention and, together with the description, explain the invention. In the drawings,

[0015] FIG. 1 illustrates an exemplary network in which systems and methods, consistent with the present invention, may be implemented;

[0016] FIG. 2 illustrates exemplary QKD relay nodes of the QKD network of FIG. 1 consistent with the present invention;

[0017] FIG. 3 illustrates exemplary QKD link metrics associated with the links between the QKD relay nodes of FIG. 2 consistent with the present invention;

[0018] FIG. 4A illustrates an exemplary shortest path for transporting end-to-end secret keys through the QKD network of FIG. 2 consistent with the present invention;

[0019] FIG. 4B illustrates exemplary disjoint paths through the QKD for transporting end-to-end secret keys through the QKD of network of FIG. 2 consistent with the present invention;

[0020] FIG. 5A illustrates an exemplary configuration of a QKD relay consistent with the

present invention;

[0021] FIG. 5B illustrates an exemplary configuration of a quantum cryptographic link interface of the QKD relay of FIG. 5A consistent with the present invention;

[0022] FIG. 6 illustrates an exemplary QKD neighbor database associated with the QKD relay of FIG. 5A consistent with the present invention;

[0023] FIG. 7 illustrates an exemplary configuration of the QKD neighbor database of FIG. 6 consistent with the present invention;

[0024] FIG. 8 illustrates an exemplary link state advertisement for disseminating link metrics consistent with the present invention;

[0025] FIG. 9 is a flow chart that illustrates an exemplary QKD link metric determination process consistent with the present invention; and

[0026] FIG. 10 is a flow chart that illustrates an exemplary process for determining one or more paths for transporting end-to-end secret keys via quantum cryptographic mechanisms consistent with the present invention.

DETAILED DESCRIPTION

[0027] The following detailed description of the invention refers to the accompanying drawings. The same reference numbers in different drawings may identify the same or similar elements. Also, the following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims and their equivalents.

[0028] Systems and methods consistent with the present invention provide mechanisms for routing secret encryption/decryption keys across a QKD network. Routing, consistent with the present invention, may use link metrics derived, in some implementations, from a

number of secret key bits exchanged between each node connected by a respective link. The derived link metrics may be used in a number of routing algorithms for determining at least one "best" path through the QKD network for subsequent end-to-end key transport.

EXEMPLARY NETWORK

[0029] FIG. 1 illustrates an exemplary network 100 in which systems and methods for distributing encryption keys via quantum cryptographic mechanisms, consistent with the present invention, may be implemented. Network 100 may include QKD endpoints 105a and 105b connected via sub-network 110 and QKD sub-network 115. Two QKD endpoints 105a and 105b are shown by way of example only. Network 100 may include multiple QKD endpoints 105 connected via sub-network 110 and QKD sub-network 115.

[0030] QKD endpoints 105a and 105b may each include a host or a server. QKD endpoints 105a and 105b that include servers may further connect to private enclaves 120a and 120b, respectively. Each private enclave 120 may include local area networks (LANs) (not shown) interconnected with one or more hosts (not shown). Sub-network 110 can include one or more circuit-switched or packet-switched networks of any type, including a Public Land Mobile Network (PLMN), Public Switched Telephone Network (PSTN), LAN, metropolitan area network (MAN), wide area network (WAN), Internet, or Intranet. The one or more PLMNs may further include packet-switched sub-networks, such as, for example, General Packet Radio Service (GPRS), Cellular Digital Packet Data (CDPD), and Mobile IP sub-networks.

[0031] QKD sub-network 115 may include one or more QKD relays (QKD relays 205A and 205H shown for illustrative purposes only) for transporting end-to-end secret keys

between a source QKD endpoint (e.g., QKD endpoint 105a) and a destination QKD endpoint (e.g., QKD endpoint 105b). The QKD relays of QKD sub-network 115 may include trusted relays. Trusted QKD relays may include QKD relays that consist of a known or assumed level of security.

[0032] Consistent with the present invention, each QKD relay 205 and QKD endpoint 105 of sub-network 115 may exchange secret key bits, via QKD techniques, with each of its neighboring QKD relays. For example, as shown in FIG. 1, QKD endpoint 105a, QKD relay 205A, QKD relay 205H, and QKD endpoint 105b may exchange secret key bits with each "neighbor" that may used for transporting end-to-end keys between the neighboring nodes. For example, QKD endpoint 105a and QKD relay 205A may exchange a first set of secret key bits for transporting an end-to-end key. QKD relay 205A and QKD relay 205H may exchange a second set of secret key bits for transporting an end-to-end key. QKD relay 205H and QKD endpoint 105b may exchange a third set of secret key bits for transporting an end-to-end key.

[0033] Subsequent to key transport via QKD sub-network 115, QKD endpoint 105a and QKD endpoint 105b may encrypt end-to-end traffic using the transported key(s) and transmit the traffic via sub-network 110.

[0034] FIG. 2 illustrates an exemplary diagram, consistent with the present invention, that depicts QKD relays of QKD sub-network 115. QKD sub-network 115 may include one or more QKD relays 205A – 205H interconnected via one or more links that may carry light throughout the electromagnetic spectrum, including light in the human-visible spectrum and light beyond the human-visible spectrum, such as, for example, infrared or ultraviolet light.

The interconnecting links may include, for example, conventional optical fibers. Alternatively, the interconnecting links may include free-space optical paths, such as, for example, through the atmosphere or outer space, or even through water or other transparent media. As another alternative, the interconnecting links may include hollow optical fibers that may be lined with photonic band-gap material. Sub-network 115 may consist of a mixture of such differing types of links, e.g., some links being freespace, others being through fiber, and yet others based on entanglement. As shown in FIG. 2, QKD endpoints 105a and 105b may each connect with one or more QKD relays of QKD sub-network 115. The configuration of the relays of QKD sub-network 115, and the interconnection of QKD endpoint 105a and 105b, as shown in FIG. 2, is for illustrative purposes only. More, or fewer, QKD relays 205 may exist in QKD sub-network 115, with various different links interconnecting the QKD relays 205. Additionally, each QKD endpoint 105 may have QKD links to multiple QKD relays, thus, permitting fully disjoint paths between the endpoints.

[0035] FIG. 3 illustrates a link metric diagram that depicts one or more metrics associated with each link between each QKD relay 205 of QKD sub-network 115. The one or more metrics associated with each link may be determined in a number ways, including, for example, by a function of a number of secret key bits exchanged between two relays at each end of a respective link. The one or more metrics associated with each link may be determined in other exemplary ways, including, for example, basing a link metric on rates of change in a number of secret bits shared between two relays, a time series average of a number of secret bits shared between two relays, and/or predictions of a number of shared secret bits that will be available at two relays interconnected by a respective link. In one

implementation, a metric M_{link} for each link may be determined in accordance with the following:

$$M_{LINK} = 5 + \frac{100}{q+1} \qquad \text{Eqn. (1)}$$

where q is associated with a number of shared secret bits for a given link. In some implementations, for example, q may represent a number of blocks of known size of shared secret bits. In other implementations, q may represent just the number of individual shared secret bits for the given link.

[0036] Each link of QKD sub-network 115 may have either "simplex" or "duplex" link metrics. A link with a "simplex" link metric may have a single metric for both directions along the link. A link with "duplex" link metrics may have two distinct metrics, one for each direction along the link. For example, FIG. 3 illustrates "duplex" link metrics between each QKD relay 205 of QKD sub-network 115. In FIG. 3, for example, two link metrics (i.e., D-C link metric, C-D link metric) exist between QKD relays 205C and 205D. Similarly, two link metrics (i.e., F-E link metric, E-F link metric) exist between QKD relays 205E and 205F.

[0037] FIG. 4A illustrates one implementation consistent with the invention in which a shortest path through QKD network 115, from QKD relay 205A to QKD relay 205H, is determined for transporting end-to-end secret keys via QKD. Once a node has received link metrics associated with every link between every node in QKD network 115, the node may construct an entire network graph that includes the link metrics for each link in the network. The node may then employ standard algorithms for computing the "best" paths (e.g., least cost) for key transport through QKD network 115. A wide range of conventional algorithms

exist for determining a "best" path through QKD network 115. In one implementation, for example, the conventional Shortest Path First (SPF), also known as Dijkstra's algorithm, may be employed. This algorithm allows any node in QKD network 115 to determine a single shortest path from itself to any other node in QKD network 115. For example, this algorithm permits QKD relay 205A to determine the shortest path from itself to QKD relay 205H across QKD network 115. As shown in FIG. 4A, an exemplary "best" path may include the path that includes QKD relay 205A, QKD relay 205B, QKD relay 205G and QKD relay 205H.

[0038] FIG. 4B illustrates another implementation consistent with the invention in which two or more disjoint, or partially disjoint, paths are determined for transporting end-to-end secret keys via QKD across QKD network 115 (only two disjoint paths are shown in FIG. 4B for illustrative purposes). For example, as shown in FIG. 4B, a first disjoint path may be determined that includes QKD relay 205A, QKD relay 205B, QKD relay 205C, QKD relay 205D and QKD relay 205H. A second disjoint path may be determined that includes QKD relay 205A, QKD relay 205E, QKD relay 205F, QKD relay 205G and QKD relay 205H. A number of conventional algorithms exist for determining two or more disjoint, or partially disjoint, paths through a network.

EXEMPLARY QKD RELAY

[0039] FIG. 5A illustrates components of an exemplary QKD relay 205 in which quantum cryptographic techniques can be implemented. QKD endpoints 105a and 105b may be similarly configured. QKD relay 205 may include a processing unit 505, a memory 510, an input device 515, an output device 520, one or more network interfaces 525, one or more quantum cryptographic link interfaces (QCLI 1 530-1 through QCLI-N

530-N) and a bus 535.

[0040] Processing unit 505 may perform all data processing functions for inputting, outputting, and processing of data. Memory 510 may include Random Access Memory (RAM) that provides temporary working storage of data and instructions for use by processing unit 505 in performing processing functions. Memory 510 may additionally include Read Only Memory (ROM) that provides permanent or semi-permanent storage of data and instructions for use by processing unit 505. Memory 510 can include large-capacity storage devices, such as a magnetic and/or optical recording medium and its corresponding drive.

[0041] Input device 515 permits entry of data into QKD relay 205 and includes a user interface (not shown). Output device 520 permits the output of data in video, audio, and/or hard copy format. Network interface(s) 525 interconnect QKD relay 205 with sub-network 110 via links unprotected by quantum cryptographic techniques. QCLI 530-1 through QCLI 530-N interconnect QKD relay 205 with QKD sub-network 115 via links protected by quantum cryptographic techniques. Bus 535 interconnects the various components of QKD relay 205 to permit the components to communicate with one another.

EXEMPLARY QUANTUM CRYPTOGRAPHIC LINK INTERFACE

[0042] FIG. 5B is a diagram illustrating exemplary components of a quantum cryptographic link interface QCLI 530. Other QCLI's in a QKD relay 205 may be configured similarly to QCLI 530 shown in FIG. 5B. QCLI 530 may include a photon

source 540, a phase/polarization modulator 545, a photon detector 550, a photon evaluator 555, and a bus 535.

[0043] Photon source 540 may include, for example, a conventional semiconductor laser. Photon source 540 produces photon signals according to instructions provided by processing unit 505. Phase/polarization modulator 545 may include, for example, conventional semiconductor phase modulators or conventional liquid crystal polarization modulators. Phase/polarization modulator 545 may encode outgoing photon signals from photon source 540 according to commands received from processing unit 505 for transmission across an optical link.

[0044] Photon detector 550 can include, for example, conventional avalanche photo diodes (APDs) or conventional photo-multiplier tubes (PMTs). Photon detector 550 may detect photon signals received across an optical link from other QCLI's in QKD network 115.

[0045] Photon evaluator 555 can include conventional circuitry for processing and evaluating output signals from photon detector 550 in accordance with conventional quantum cryptographic techniques.

EXEMPLARY QKD NEIGHBOR DATABASE

[0046] FIG. 6 illustrates an exemplary QKD neighbor database 600 that may be associated with a QKD relay 205 consistent with the present invention. Database 600 may be stored in memory 510 of QKD relay 205, or may be located externally to QKD relay 205. QKD neighbor database 600 may include multiple entries, such as, for example, one entry for each neighboring node. By way of example, FIG. 7 illustrates an exemplary database 600

associated with QKD relay 205B of QKD network 115. A different QKD neighbor database 600 may, though, be associated with each QKD relay 205 of QKD network 115.

[0047] Each entry of QKD neighbor database 600 may include a neighbor node identifier 705, a number of shared bits value 710, a shared secret bit pool 715 and a link metric 720. Neighbor node identifier 705 may uniquely identify a neighboring node. In some implementations, for example, identifier 705 may include a network address of the neighboring node. In the example of FIG. 7, database 600 includes entries for each of QKD relays 205A, 205C, 205E and 205G. The number of shared bits value 710 indicates the exact number of secret bits shared with the node identified by node identifier 705 via QKD. For example, the number of shared bits value 710 for QKD relay 205A may include the number of bits shared between QKD relay 205B and 205A. Shared secret bit pool 715 may contain the secret bits shared with the node identified by node identifier 705 via QKD. Link metric 720 may include a metric value associated with a "length" or "cost" of a link identified by the corresponding neighbor node ID 705. For example, as shown in FIG. 7, a link metric of M_{L_A} may be associated with the link between QKD relay 205B and QKD relay 205A identified by neighbor node ID 705.

EXEMPLARY LINK STATE ADVERTISEMENT

[0048] FIG. 8 illustrates an exemplary link state advertisement that may be used by a QKD relay for advertising the link metrics of each link connected to the QKD relay. Link state advertisement 800 may include an originating node identifier 805, a sequence number 810, a number of QKD neighbors value 815 and QKD link metrics 820. Originating node identifier 805 may include a unique identifier associated with the node that originated

advertisement 800. In some implementations, for example, identifier 805 may include a network address associated with the node that originated the advertisement 800. Sequence number 810 may include a value that identifies a sequential number that advertisement 800 represents in a sequence of advertisements. Number of QKD neighbors 815 identifies a number of nodes that neighbor the node that originated advertisement 800. For example, if QKD relay 205B of FIG. 2 originates a link state advertisement, the # of QKD neighbors 815 may indicate four neighboring nodes – QKD relay 205A, QKD relay 205C, QKD relay 205E and QKD relay 205G. QKD link metrics 820 indicate a link metric for each link connected to a neighboring node. For example, if QKD relay 205B of FIG. 2 originates a link state advertisement, QKD link metrics 820 may include four link metrics: a B-A link metric indicating the metric of the link between QKD relay 205B and QKD relay 205A, a B-C link metric indicating the metric of the link between QKD relay 205B and QKD relay 205C, a B-E link metric indicating the metric of the link between QKD relay 205B and QKD relay 205E and a B-G link metric indicating the metric of the link between QKD relay 205B and QKD relay 205G.

EXEMPLARY LINK METRICS DETERMINATION PROCESS

[0049] FIG. 9 is a flowchart that illustrates an exemplary process, consistent with the present invention, for determining link metrics of links connecting a QKD relay 205 with neighboring QKD relays. As one skilled in the art will appreciate, the method exemplified by FIG. 9 can be implemented as a sequence of instructions and stored in a respective memory 510 of each QKD relay 205 for execution by a respective processing unit 505.

[0050] The exemplary process may begin with the exchange of secret key bits with

neighboring nodes (i.e., QKD relays and QKD endpoints) of QKD network 115 via quantum key distribution [act 905]. For example, as shown in FIG. 2, QKD relay 205B may exchange a first set of key bits with QKD relay 205A, a second set of key bits with QKD relay 205C, a third set of key bits with QKD relay 205E and a fourth set of key bits with QKD relay 205G via QKD. The new secret bits shared with each of the neighboring nodes may be accumulated in a respective pool of shared secret bit pools 715 [act 910]. For example, the sets of key bits exchanged with QKD relay 205B may be accumulated in a respective shared secret bit pool of QKD neighbor database 600.

[0051] A current link metric of each link with each respective neighboring node may be determined based on a number of shared secret bits 710 in a corresponding pool of shared secret bit pools 715 [act 915]. For example, a number of shared secret bits 710 for neighbor QKD relay 205A may be retrieved from QKD neighbor database 600 and a link metric may be assigned to the link between QKD relay 205B and QKD relay 205A based on the retrieved number of shared secret bits 710. Metrics associated with each link may determined in a number ways, including, for example, as a function of the number of currently available secret key bits exchanged between two relays at each end of a respective link. The one or more metrics associated with each link may be determined in other exemplary ways, including, for example, basing a link metric on rates of change in a number of secret bits shared between two relays, a time series average of a number of secret bits shared between two relays, and/or predictions of the number of shared secret bits that will be available at two relays interconnected by a respective link. In one implementation, a metric M_{link} for each link may be determined in accordance with Eqn (1):

$$M_{LINK} = 5 + \frac{100}{q+1}$$

where q is associated with a number of shared secret bits for a given link. In some implementations, for example, q may represent a number of blocks of known size of shared secret bits. In other implementations, q may represent just the number of individual shared secret bits for the given link. The determined link metrics may then be stored [act 920]. The determined link metrics may be stored, for example, as link metric values 720 in QKD neighbor database 600.

[0052] The determined link metrics may further be disseminated [act 925] via, for example, a link state advertisement 800. Before disseminating link state advertisement 800, an originating node identifier 805 and an appropriate sequence number 810 may be inserted in advertisement 800. Additionally, each link metric associated with a link to a neighboring node may be inserted in the QKD link metrics 820 portion of link state advertisement 800. In some implementations consistent with the invention, the determined link metrics may be reliably "flooded" to neighboring QKD relays. In other implementations consistent with the invention, the determined link metrics may be disseminated to a centralized "route server," which may subsequently be queried by any given node in QKD network 115 to determine a link metric associated with a particular link. In some implementations, for example, a link state advertisement 800 may be disseminated if an entire pool of shared secret bits suddenly runs low such that other nodes in QKD network 115 can be informed that the link metric has changed significantly for that particular link. A link state advertisement 800 may be disseminated periodically. In some implementations, a link state advertisement 800 may be

disseminated asynchronously.

EXEMPLARY KEY TRANSPORT PATH DETERMINATION PROCESS

[0053] FIG. 10 is a flowchart that illustrates an exemplary process, consistent with the present invention, for determining a secret key transport path through QKD network 115. As one skilled in the art will appreciate, the method exemplified by FIG. 10 can be implemented as a sequence of instructions and stored in memory 510 of QKD relay 205 for execution by processing unit 505.

[0054] The exemplary process may begin with the receipt of link metrics from neighboring nodes in QKD network 115 [act 1005]. Link metrics may be received in link state advertisements 800 sent from other nodes in QKD network 115. Each received link metric may be stored, for example, in a link metric value 720 of QKD neighbor database 600 [act 1010]. A QKD network graph may then be constructed using the stored link metrics [act 1015]. Conventional graph algorithms may be used for constructing a graph of QKD network 115 using the stored link metrics. One or more paths may then be determined to every node in QKD network 115 for key transport using the constructed QKD network graph [act 1020]. The one or more paths may be determined using conventional path determination algorithms, such as, for example, the Shortest Path First (SPF) algorithm. Other conventional algorithms, though, may be equivalently used, such as, for example, conventional algorithms that determine two or more disjoint, or partially disjoint, paths through a network. Subsequent to the determination of one or more paths to every node in QKD network 115, secret keys may be transported over the determined one or more paths. In some implementations, for example, key transport may be implemented as described in the related and above-noted co-

pending Application No. _____ (Attorney Docket No. 03-4018), entitled "Systems and Methods for Implementing Routing Protocols for Quantum Cryptographic Key Transport."

CONCLUSION

[0055] Systems and methods consistent with the present invention, therefore, provide mechanisms for routing end-to-end keys across a QKD network. Routing algorithms, consistent with the present invention, may employ link metrics associated with each link of the QKD network that can be determined based on a number of secret key bits exchanged between each node connected by a respective link. The determined link metrics may then be disseminated throughout the network so that conventional graph theory algorithms may be employed to determine one or more paths through the QKD network. The determined one or more paths may be used for transporting end-to-end keys that can be used by QKD endpoints for encrypting/decrypting data sent across a public channel.

[0056] The foregoing description of implementations of the present invention provides illustration and description, but is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. For example, instead of a single centralized "route" server, used in some implementations as described above, for storing link metrics and determining paths through QKD sub-network 115, multiple redundant "route" servers may be employed. Additionally, a hierarchical or "regional" set of "route" servers may be employed for large QKD networks. Furthermore, though some implementations of the present invention have been described as using link-state protocols, other non-link state

routing protocols, such as, for example, distance vector, RIP, BGP, PNNI, or so called "on demand" protocols, such as AODV and DSR, may be employed.

[0057] While series of acts have been described in FIGS. 9-10, the order of the acts may vary in other implementations consistent with the present invention. Also, non-dependent acts may be performed in parallel. No element, act, or instruction used in the description of the present application should be construed as critical or essential to the invention unless explicitly described as such. Also, as used herein, the article "a" is intended to include one or more items. Where only one item is intended, the term "one" or similar language is used.

[0058] The scope of the invention is defined by the following claims and their equivalents.